

Настройка резервного копирования

Варианты резервных копий

Senhasegura предоставляет следующие варианты резервного копирования:

- **Резервное копирование секретов (Break the glass).** Такая резервная копия может храниться во внешней среде - все пароли в ней зашифрованы мастер-паролем. В экстренной ситуации можно будет вскрыть такую резервную копию через ритуал восстановления мастер-ключа. Резервная копия паролей не используется для восстановления системы. Она нужна для доступа клиента к паролям учетных данных в случае полной недоступности решения Senhasegura.
- **Резервное копирование системы.** Содержит в себе системную информацию: данные, настройки Senhasegura, настройки среды, в которой она работает, программы, приложения и записи доступа. Такая копия может периодически копироваться в резервный репозиторий клиента в соответствии с политиками его безопасности. Этот тип резервного копирования требует длительного времени восстановления и дополнительного дискового пространства.
- **Резервное копирование видео прокси сессий.** Резервная копия видеозаписей подключения через прокси Senhasegura, зашифрованные мастер-ключом.

Резервное копирование секретов и системы создается, когда опция резервного копирования включена и настроена. Для резервного копирования видео прокси сессий необходимо выбрать «Да» в окне «**Enable sessions file backup?**».



Если система потеряет доступ к удаленному каталогу резервного копирования, вам будет отправлено уведомление по электронной почте и в SIEM.

Подключение резервного раздела

Если вы хотите, чтобы резервная копия была создана в разделе удаленного диска, перейдите в **Orbit Config Manager → Settings → Backup**; вы можете настроить его через CIFS или NFS или прямую отправку с помощью rsync. Выберите «Да» в окне «**Mount a remote partition?**».

Резервное копирование через CIFS или NFS

Для создания резервных копий Senhasegura через CIFS или NFS:

1. Выберите **Mounting a remote partition** (via CIFS or NFS).
2. Нажмите на **Add remote partition**.
3. В окне **Add remote partition**, заполните поля **Remote host** и **Remote path** информацией о сервере, где senhasegura сохранит созданную резервную копию. Например,
 - **Remote host:** myserver.com или 10.10.1.5
 - **Remote path:** /files/backup/senhasegura
4. Выберите протокол:
 - Samba (CIFS): потребуется пользователь с правами записи в каталог в **Remote path**, иначе Senhasegura не сможет создать резервную копию. При необходимости добавьте имя домена, если этого требует ваш хост-сервер.
 - Network File System (NFS): при выборе NFS обязательно разрешите IP-адрес Senhasegura в конфигурациях Remote Host NFS, иначе Senhasegura не сможет создать резервную копию.



Вы можете использовать зарегистрированные учетные данные в качестве метода аутентификации. Для этого откройте **Settings → System parameters → System parameters → Application** и выберите нужные учетные данные в поле **Remote backup credential**.



Пароли от удаленных хранилищ не должны содержать символы \, &, и !

Резервное копирование через rsync

Требования

- Наличие пользователя с разрешением на запуск rsync на целевом устройстве резервного копирования.
- Создать каталог для резервной копии, владельцем которого является пользователь rsync, например, /home/senhauser/backup_rsync
- Установить пакет sync на сервере резервного копирования.

Чтобы Senhasegura создавала резервные копии через rsync, необходимо настроить rsync и предоставить доступ к серверу резервного копирования с открытым ключом.



Резервное копирование rsync выполняется с аутентификацией с использованием SSH-ключа. Вам нужно будет настроить отдельного пользователя на вашем сервере и положить его открытый ключ в «authorized_keys».

Настройка резервного копирования через rsync

Шаг 1 - Настройка резервного копирования системы Senhasegura

1. Выберите **Send to a remote Linux server (via RSYNC)**.
2. Добавьте **User** сервера резервного копирования, который будет использоваться Senhasegura.
3. Добавьте имя хоста или IP-адрес резервного сервера, например, myserver.com или 10.10.1.5.
4. Добавьте каталог **Remote path** чтобы сохранить резервное копирование. Например, "/files/backup/senhasegura".

Шаг 2 - Резервная копия учетных данных Senhasegura

1. Откройте **Orbit → Settings → Backup menu**.
2. Включите резервное копирование системы и видео.
3. Настройте удаленный раздел с помощью rsync.
4. Введите имя пользователя, IP-адрес устройства и полный путь к созданной папке резервного копирования.

Шаг 3 - Копирование открытого ключа пользователя

1. Войдите на главный узел Senhasegura, используя **SSH**, порт **59022**, с пользователем **mt4adm**.
2. Соберите открытый ключ, этой командой :

```
sudo cat /root/.ssh/id_rsa.pub
```

3. Скопируйте открытый ключ с вашего терминала.
4. Войдите на используемый сервер резервного копирования и добавьте открытый ключ в файл «authorized_keys» от пользователя, указанного в поле **User** во время настройки Senhasegura rsync.
5. Вставьте скопированный открытый SSH-ключ корневого пользователя главного экземпляра Senhasegura в файл authorized_keys целевого устройства.

```
vim /home/rsync/.ssh/authorized_keys
```

Шаг 4 - Тестовое резервное копирование через rsync

1. Войдите на сервер Senhasegura, используя **SSH**, порт **59022**, с пользователем **mt4adm**.
2. Выполните следующую команду:

```
sudo orbit backup create
```

3. Вы получите подтверждение от rsync и информацию о расчетной продолжительности передачи данных.
4. Проверьте, находятся ли файлы теперь в **Remote path** на сервере резервного копирования.

Файл журнала резервного копирования

Чтобы проверить журнал резервного копирования:

1. Войдите на сервер Senhasegura, используя **SSH**, порт **59022**, с пользователем mt4adm.
2. Запустите следующую команду:

```
tail -f /var/log/orbinibkp.log
```

Версия #4

Денис Морозов создал 30 марта 2023 17:09:43

Денис Морозов обновил 18 апреля 2023 17:49:08